

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

DANIEL STRATMAN,

Defendant.

4:13-CR-3075

MEMORANDUM AND ORDER

This matter is before the Court on the defendant's motion to dismiss (filing [6](#)), the Magistrate Judge's findings and recommendation (filing [16](#)) that the motion be denied, and the defendant's objection (filing [18](#)) to the Magistrate Judge's findings and recommendation. The Court will overrule the defendant's objection, adopt the Magistrate Judge's findings and recommendation, and deny the defendant's motion to dismiss.

As relevant, the defendant is charged with violating [18 U.S.C. § 1030\(a\)\(5\)\(A\)](#), which provides punishment for anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." The defendant's argument is premised on the claim that he "was authorized to access the protected computer, and used that authorization to access data in the computer for which he was not authorized, thereby exceeding his authorization." Filing [23](#) at 1. The defendant argues that while he admittedly exceeded the scope of his authorized access, he did not act "without authorization" within the meaning of [§ 1030\(a\)\(5\)\(A\)](#) because his *initial* access to the system was authorized.

In other words, the defendant claims that [§ 1030\(a\)\(5\)\(A\)](#) "cannot be criminally violated by one who was authorized to access the computer at the time he caused the alleged damage." Filing [23](#) at 2. As the Magistrate Judge's findings and recommendation persuasively explain, the defendant's reading of the statute is unsupported. The phrase "without authorization" modifies the phrase "intentionally causes damages": that is, one who is authorized to access a system, but not authorized to damage it, violates the statute by intentionally damaging it "without authorization."

The defendant argues that the Magistrate Judge erred because the phrase "without authorization" refers to "the element of access to the protected computer." Filing [23](#) at 3. The defendant asserts that it is "manifest

that an essential element of a violation of the Act would be that the person access the protected computer without authorization or by exceeding the authorization given." Filing 23 at 3. But that is not obvious at all, particularly in context. Section 1030(a)(5) provides punishment for one who

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(Emphasis in original.) It is apparent from § 1030(a)(5)(B) and (C) that Congress knew exactly how to require proof that a defendant's access to a computer was unauthorized. "[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Dean v. United States*, 556 U.S. 568, 573 (2009) (quoting *Russello v United States*, 464 U.S. 16, 23 (1983)).

There is, in fact, nothing in § 1030(a)(5)(A) to suggest that access to a protected computer is an element of the offense at all, whether or not it was authorized. Nor is that surprising: it is possible for a perpetrator to damage a computer system by distributing a computer virus, for instance, without ever directly accessing the damaged system. The fact that the defendant in this case did access the system, with authorization, does not change the fact that if he intentionally damaged the system without authorization, he may be charged with violating § 1030(a)(5)(A).

Although the Court finds that result to be compelled by the plain language of the statute, the Court also notes support for its conclusion in the legislative history. The Senate Judiciary Committee's report on the bill containing the relevant provision explains:

Specifically, as amended, subsection 1030(a)(5)(A) would penalize, with a fine and up to 5 years' imprisonment, anyone who knowingly causes the transmission of a program,

information, code or command and intentionally causes damage to a protected computer. *This would cover anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer.* Subsection 1030(a)(5)(B) would penalize, with a fine and up to 5 years' imprisonment, anyone who intentionally accesses a protected computer without authorization and, as a result of that trespass, recklessly causes damage. This would cover outside[] hackers into a computer who recklessly cause damage. Finally, subsection 1030(a)(5)(C) would impose a misdemeanor penalty, of a fine and up to 1 year imprisonment, for intentionally accessing a protected computer without authorization and, as a result of that trespass, causing damage. This would cover outside hackers into a computer who negligently or accidentally cause damage.

In sum, under the bill, *insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage.* By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.

The rationale for this difference in treatment deserves explanation. Although *those who intentionally damage a system, without authority, should be punished regardless of whether they are authorized users*, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. . . . [I]t is better to ensure that section 1030(a)(5) criminalizes all computer trespass, *as well as intentional damage by insiders*, albeit at different levels of severity.

S. Rep. No. 104-357, at 10-11 (1996) (emphasis supplied). In short, both the language of the statute and the legislative history support the conclusion that unauthorized access to the protected computer system is *not* an element of the offense defined by § 1030(a)(5)(A).

The defendant reasserts his contention that the phrase "without authorization" should not be related to the phrase "intentionally causes damage" because it would not make sense for someone to be authorized to cause damage. The Magistrate Judge's rejection of that point was persuasive, and the Court need not restate it. Anyone who has ever redecorated a home,

for instance, is familiar with the basic principle that sometimes "damage" is necessary to facilitate reconstruction or improvement. In the context of information technology, the simplest example may be clearest: old files get deleted all the time.

The defendant also attempts, at length, to distinguish the cases relied upon by the Magistrate Judge. The Court will not address his attempts at length: while the cases are not precisely on point, the Magistrate Judge was not contending that they were, and the Magistrate Judge's discussion of that authority made the varying relevance and weight of the cases clear. And distinguishing other cases does not make the defendant's reading of the statutory language more persuasive, nor does it change the fact that the defendant has produced *no* cases supporting his construction of the statute.

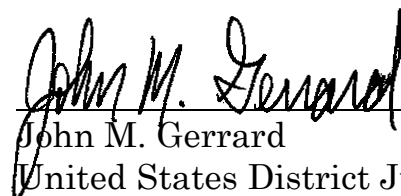
Finally, the defendant relies on the principle that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." See *Liparota v. United States*, 471 U.S. 419, 427 (1985). For the reasons explained above and by the Magistrate Judge, the Court does not find any ambiguity in § 1030(a)(5)(A) to resolve. The Court will therefore overrule the defendant's objection, adopt the Magistrate Judge's findings and recommendation, and deny the defendant's motion to dismiss.

IT IS ORDERED:

1. The defendant's objection (filing 18) is overruled.
2. The Magistrate Judge's findings and recommendation (filing 16) are adopted.
3. The defendant's motion to dismiss (filing 6) is denied.

Dated this 18th day of October, 2013.

BY THE COURT:

  
\_\_\_\_\_  
John M. Gerrard  
United States District Judge